4. Sigurnosni mehanizmi operacijskog sustava

Jedanaesto poglavlje u udžbeniku L. Budin, M. Golub, D. Jakobović, L. Jelenković, Operacijski sustavi

Sadržaj

4.1. Osnovni pojmovi

- Sigurnosne prijetnje i napadi
- Sigurnosni zahtjevi
- Primjeri napada
- Sigurnosni mehanizmi OS-a

4.2. Autentifikacija

- MAC
- Autentifikacijsko kriptiranje
- Digitalni potpis

4.3. Sigurnosni protokoli

- Razmjena ključeva
- Raspodjela ključeva
- Autentifikacijski protokoli

4.4. Kontrola pristupa

- Autorizacija
- Prijava za rad
- Autentifikacijski protokol Kerberos

4.5. Infrastruktura javnog ključa

- Dijelovi PKI
- Digitalni certifikat
- X.509 autentifikacijski protokoli

4.6. Sigurnosna stijena

4.1. Osnovni pojmovi

Sigurnosne prijetnje i napadi

Sigurnosni zahtjevi

Primjeri napada

Sigurnosni mehanizmi OS-a

Ponavljanje: Sigurnosni zahtjevi

Osnovni sigurnosni zahtjevi	1. tajnost 2. autentičnost 3. neporecivost 4. integritet
Dodatni sigurnosni zahtjevi	5. kontrola pristupa 6. raspoloživost

Ponavljanje: Sigurnosni zahtjevi

Osnovni sigurnosni zahtjevi

povjerljivost

štiti informacije od neautoriziranog pristupa

1. tajnost
2. autentičnost

3. neporecivost
4. integritet

Dodatni sigurnosni zahtjevi

5. kontrola pristupa
6. raspoloživost

Ponavljanje: Sigurnosni zahtjevi

povjerljivost
Confidentiality

1. tajnost
2. autentičnost

Integrity

4. integritet

Availability

5. kontrola pristupa
6. raspoloživost

Ponavljanje: Sigurnost sustava

Sustav je siguran kada se njegovi resursi koriste i pristupa im se na za to predviđen način u svim okolnostima.

- nedostižno

Primjeri napada na sigurnost sustava

- neautorizirano čitanje podataka – narušena povjerljivost
- neautorizirana modifikacija podataka – narušen integritet
- neautorizirano brisanje podataka – narušena raspoloživost
- napad uskračivanjem usluge – narušena raspoloživost
- krađa usluge – narušeni povjerljivost i integritet

Ponavljanje: Osnovni kriptografski pojmovi

Kriptiranje vs. šifriranje

- Kerckhoffov princip: Kriptosustav mora biti siguran i onda kada su sve informacije o kriptosustavu javno poznate, osim tajnog ključa.

Podjela kriptografskih algoritama

- simetrični algoritmi
  - AES, DES, 3DES, IDEA
- asimetrični algoritmi
  - RSA, ECC, ElGamal
- funkcije za izračunavanje sažetka (*hash*)
  - SHA-1, SHA-2, SHA-3

ranjivosti i napadi	razine	zaštita
logičke greške, propusti u dizajnu, umetanje koda	programi	pokretanje u zaštićenom okruženju
nepravilno podešene postavke sustava, propusti u sustavu	OS	redovito ažuriranje sustava, rekonfiguracija postavki sustava
prisluškivanje, lažno predstavljanje	mreža	sigurnosni štit (*firewall*) kriptiranje, autentifikacija
pristup računalu, napadi na sklopovlje, napadi koji koriste sporedna svojstva	fizička razina	kriptiranje na nivou uređaja, zaštitari, zaštićene prostorije

Sigurno programiranje

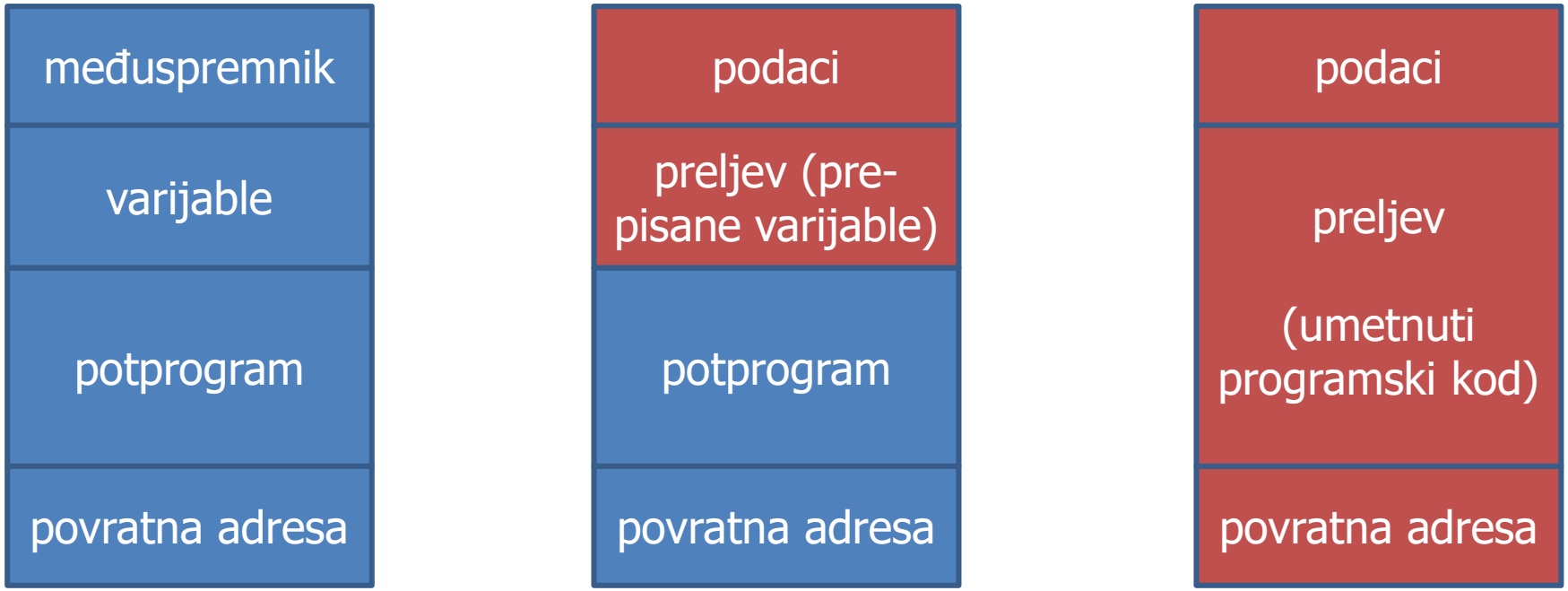
- veliki izazov
- primjer programa koji ima problema s preljevom međuspremnika (*buffer-overflow*):

```
#include <stdio.h>
#define BUFFER SIZE 256
int main(int argc, char *argv[]){
   char buffer[BUFFER SIZE];
   if (argc < 2)
        return -1;
   else {
        strcpy(buffer,argv[1]);
        return 0;
   }
}
```

- pomaže kada programeri međusobno pregledavaju programe (*code review*) tražeći logičke pogreške

Moguće posljedice napada umetanjem koda

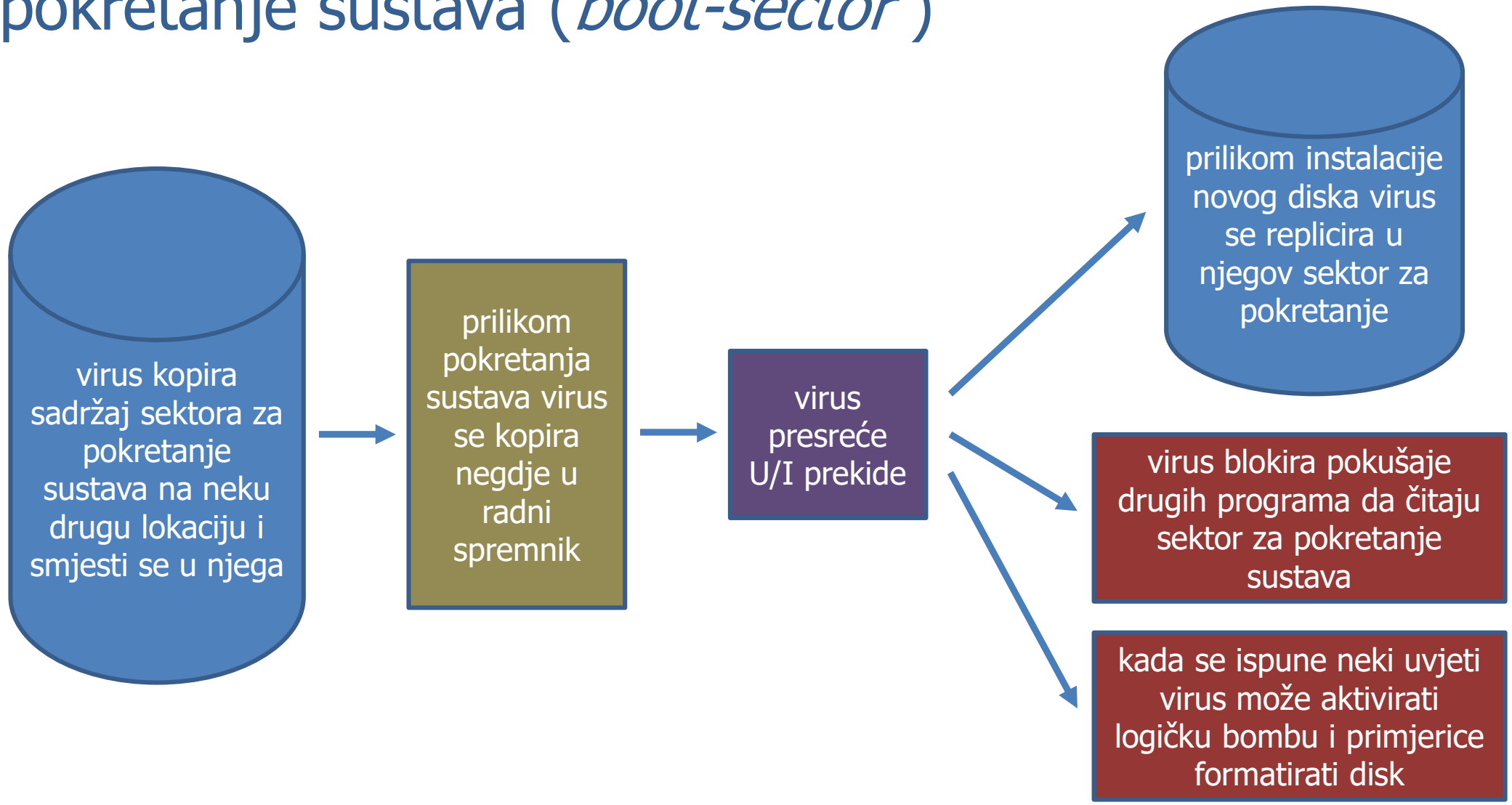
- engl. code injection



zamjena sadržaja varijabli

povratna adresa je adresa zloćudnog programa

Primjer računalnog virusa smještenog u sektor za pokretanje sustava (*boot-sector*)



Sigurnosni mehanizmi OS-a

- Kontrola pristupa
  - fundamentalni sigurnosni mehanizam OS-a
  - čemu sve pojedini proces smije pristupiti
  - upravljanje pravima pristupa
- Autentifikacija
  - prilikom prijave
  - za svaki proces zna se čiji je
- Vođenje dnevnika (engl. *logging*)
  - nadzor, otkrivanje propusta, forenzika, oporavak od pogrešaka
- Kriptiranje datotečnog podsustava
- Ažuriranje operacijskog sustava

4.2. Autentifikacija poruka

MAC

Autentifikacijsko kriptiranje

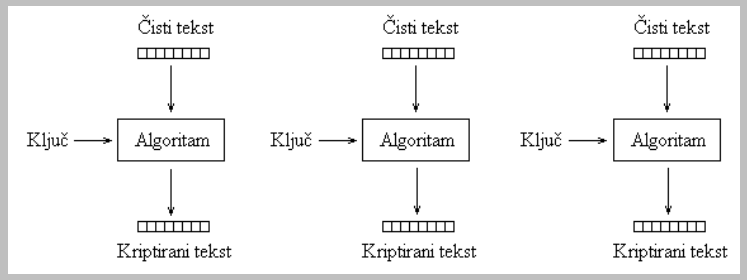
Digitalni potpis

Autentifikacija

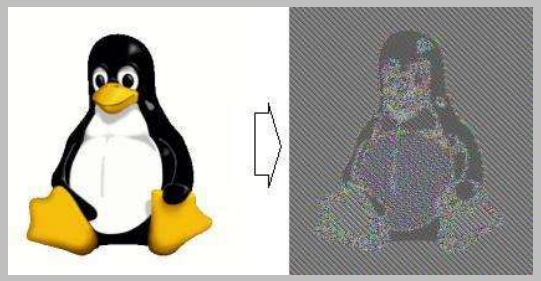
- korisnika
  - Prijava za rad
  - time ćemo se baviti naknadno
- poruka
  - načinima kriptiranja MAC (*Message Authentication Code*) i HMAC
  - hibridnim postupcima EtM, E&M, MtE te načinom kriptiranja GCM ako želimo uz autentičnost osigurati i tajnost
  - autentifikacijsko kriptiranje osigurava tajnost i autentičnost
  - digitalni potpis osigurava autentičnost, integritet i neporecivost
    - digitalni pečat osigurava i tajnost
    - autentičnost se u PKI sustavu utvrđuje certifikatom

Načini kriptiranja

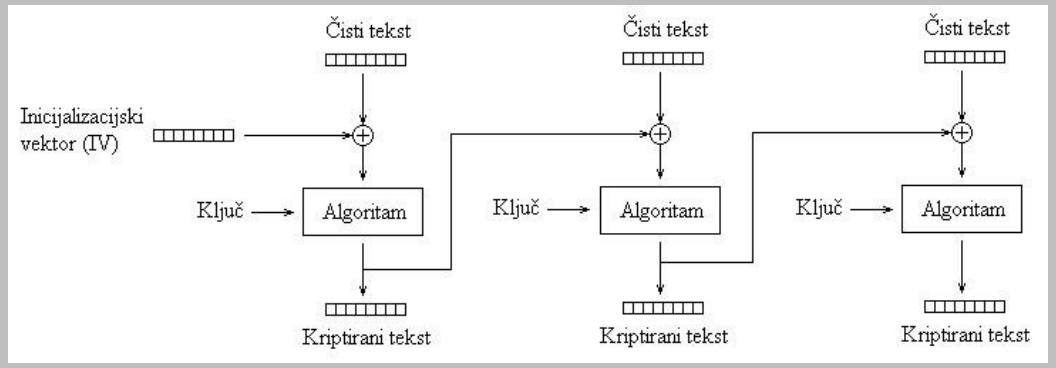
ECB



cilj je onemogućiti da isti blokovi jasnog teksta daju isti blok kriptiranog teksta ...

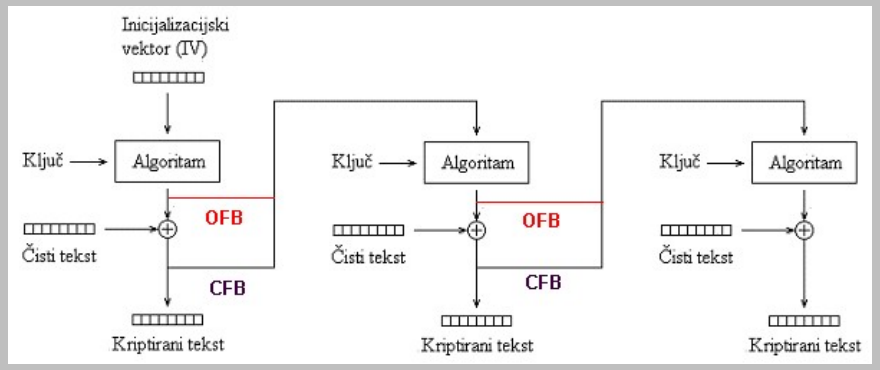


CBC

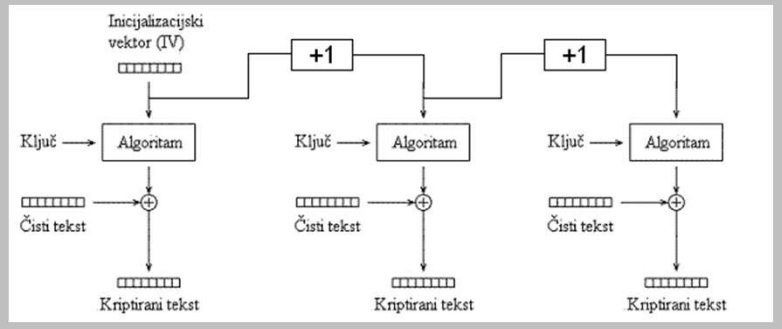


... te da se blok simetrični algoritmi mogu koristiti za kriptiranje toka podataka

CFB i OFB



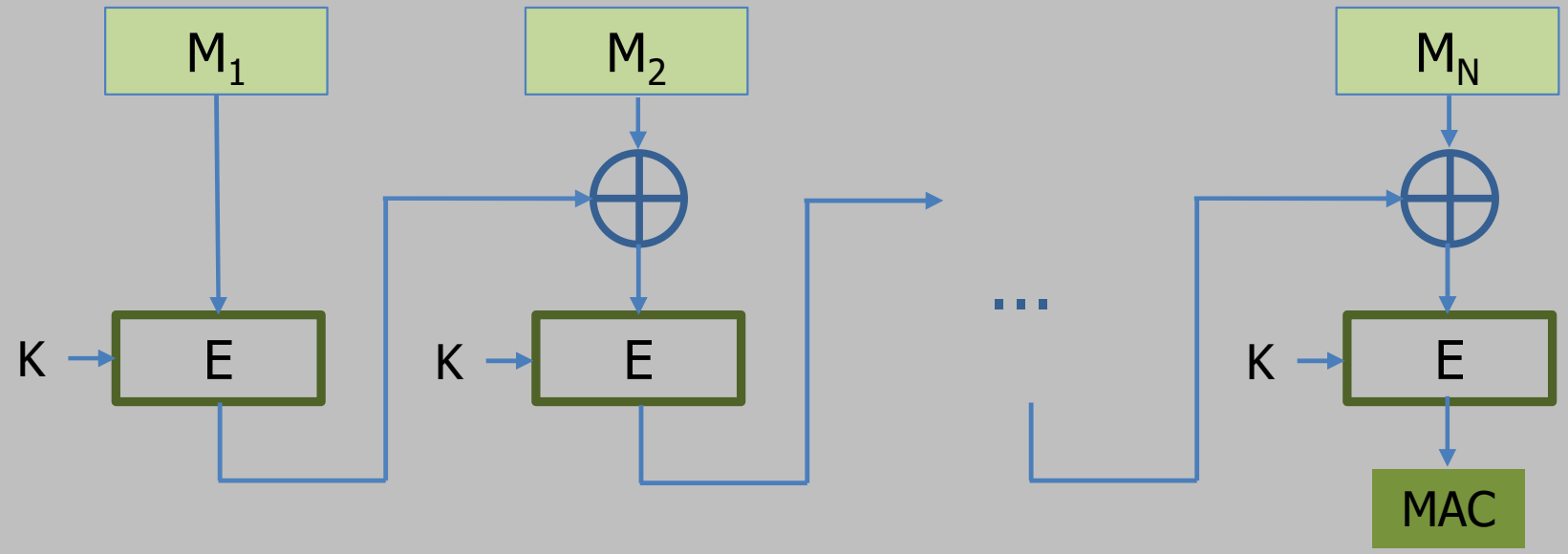
CTR



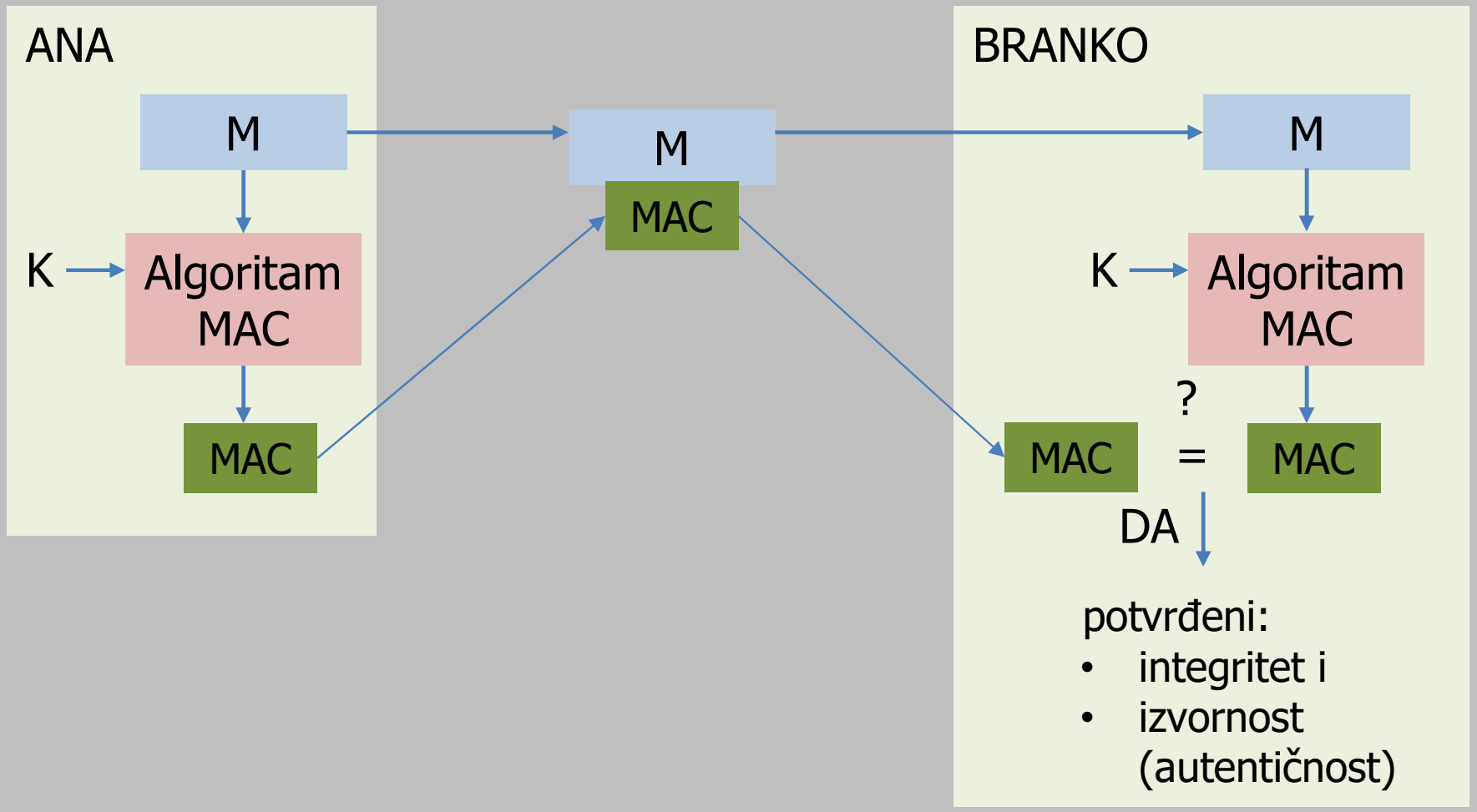
Način kriptiranja koji osigurava autentičnost i integritet MAC (*Message Authentication Code*)

- autentičnost pošiljatelja osigurava se simetričnim kriptiranjem
  - poruku je zaštitio netko od onih koji imaju tajni ključ K

CBC-MAC:



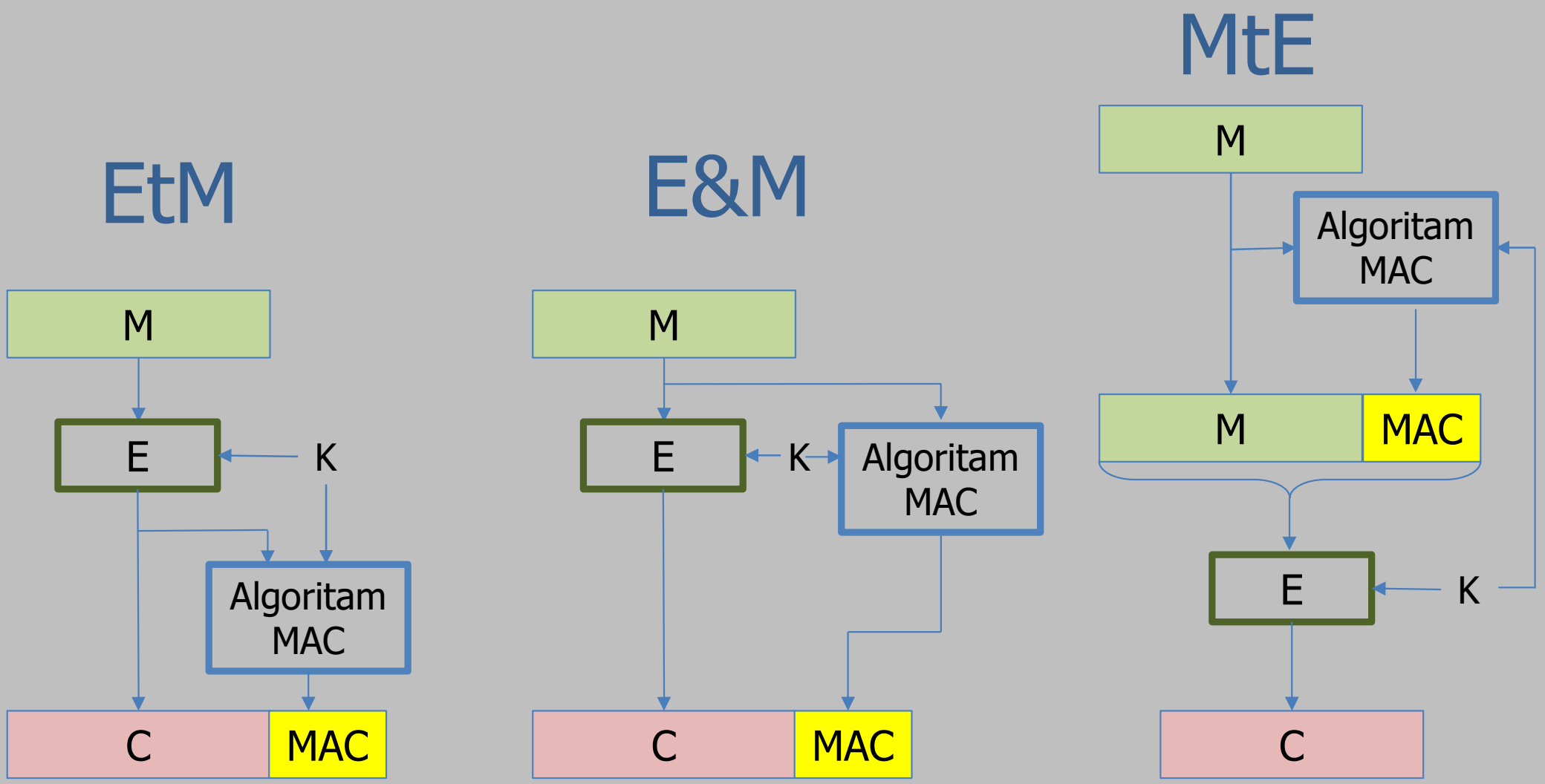
Primjer kako se može koristiti dodatak poruci MAC



Način kriptiranja koji osigurava autentičnost HMAC

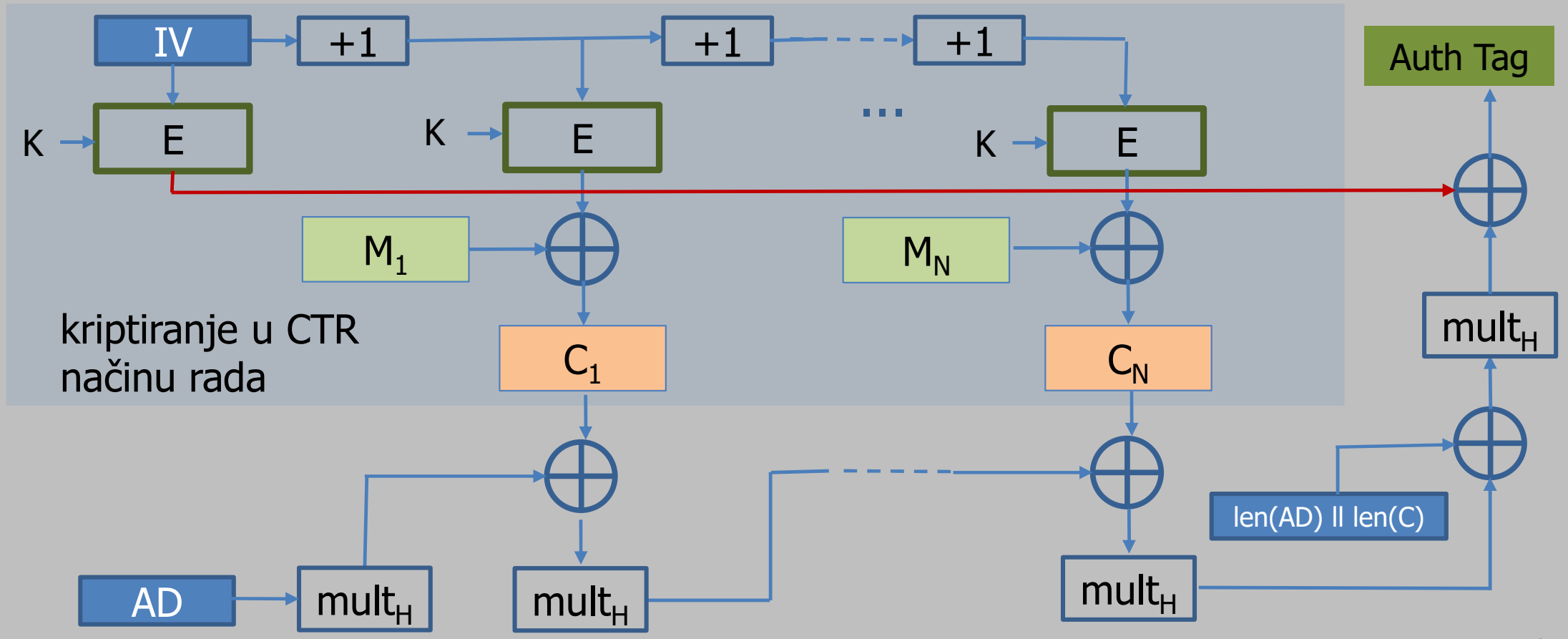
- umjesto blok simetričnog algoritma koristi funkciju za izračunavanje sažetka poruke
- *keyed-Hash Message Authentication Code*
  - HMAC_MD5
  - HMAC_SHA1
  - HMAC_SHA256
  - HMAC_SHA3
- $HMAC(K,M) = H\{(K' \oplus opad) \,||\, H[(K' \oplus ipad) \,||\, M]\}$
  - K' = H(K) ako je K veći od veličine bloka, inače K' = K
  - konstanta *opad (outer padding*) = 0x5c5c5c...5c5c
  - konstanta *ipad* (*inner padding*) = 0x363636...3636
  - *opad* i *ipad* su veličine jednog bloka

Kako uz integritet i autentičnost osigurati i tajnost?



GCM - *Galois/Counter Mode*

- način autentifikacijskog kriptiranja koji osigurava autentičnost i tajnost, a primjenjiv je samo za simetrične blok algoritme s veličninom bloka 128 bita
- varijanta *Galois Message Authentication Code, GMAC* – samo za autentifikaciju



Autentifikacijska kriptografija

- Natječaj CAESAR (*Competition for Authenticated Encryption: Security, Applicability, and Robustness*)
  - nedostatak klasičnih autentifikacijskih kriptografskih shema poput *EtM, E&M i MtE* je upravo u primjeni više algoritama
  - završio 20.3.2019. objavljeno 3 pobjednika u 3 kategorije i 5 rezervna algoritma

- NIST-ov natječaj za novi algoritam prilagođen okruženju s ograničenim računalnim resursima (*lightweigt cryptography*)
  - algoritam treba osim simetričnog uključivati i autentifikacijsko kriptiranje (*Authenticated Encryption with Associated Data*, AEAD)
  - natječaj je u tijeku

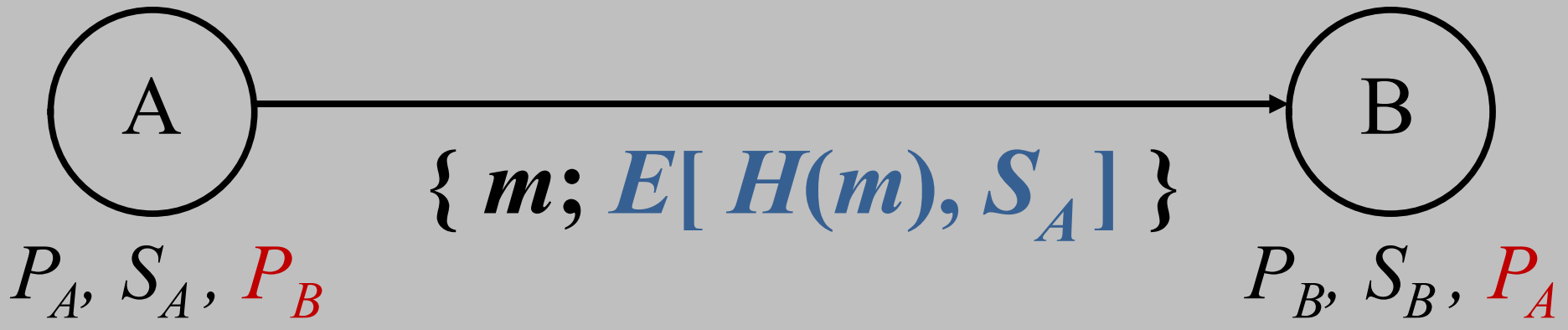
Pobjednici na natječaju CAESAR

Pobjednici su birani u tri kategorije:

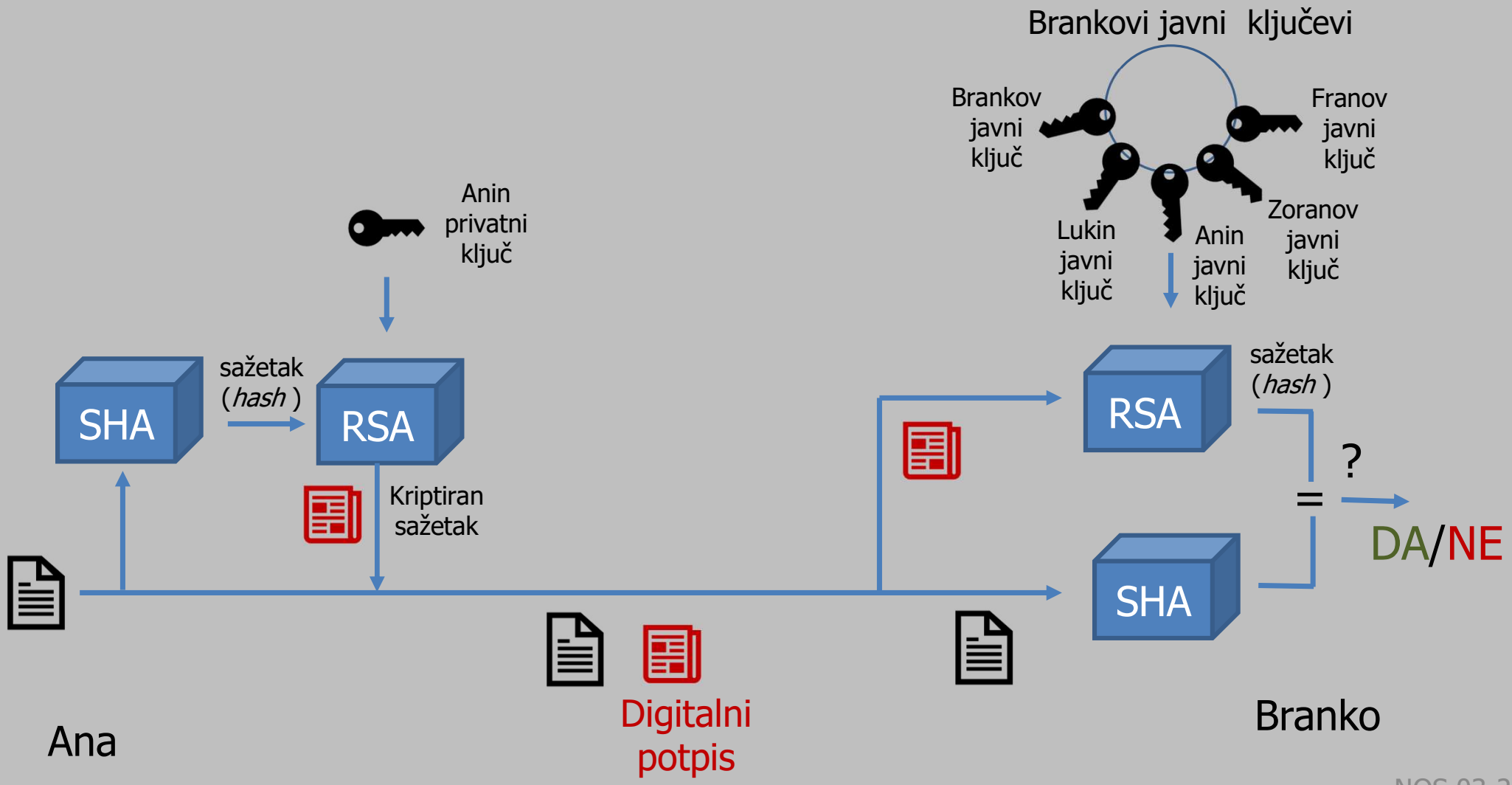
1. Algoritmi koji su najmanje zahtjevni na računalne resurse (*Lightweight applications - resource constrained environments*)
   - prvi izbor: Ascon (web)
   - drugi izbor: ACORN
2. Algoritmi visokih performansi (*High-performance applications*)
   - prvi izbor: AEGIS-128
   - drugi izbor: OCB
3. Sigurnost (*Defense in depth*)
   - prvi izbor: Deoxys-II
   - drugi izbor: COLM ili AES-COPA ili ELmD

Digitalni potpis

- dodatak poruci koji služi za
  - utvrđivanje besprijekornosti informacije (integritet i neporecivost) i za
  - identifikaciju pošiljatelja (autentičnost)
- ne osigurava tajnost!



Digitalni potpis
Postupak potpisivanja i provjere



Digitalna omotnica

- osigurava tajnost
- pošiljatelj kriptira poruku proizvoljnim ključem K simetričnim algoritmom kriptiranja
- simetrični (sjednički ili tajni) ključ K se kriptira javnim ključem primatelja P_B
- kriptirana poruka i kriptirani ključ čine digitalnu omotnicu

Digitalni pečat (1/2)

- digitalni pečat osigurava četiri sigurnosna zahtijeva:
  - tajnost
  - autentičnost
  - integritet i
  - neporecivost
- digitalni pečat je digitalno potpisana digitalna omotnica

$$\{ E(m,K); E(K,P_B) \}; \; E\{ H[E(m,K); E(K,P_B)], S_A \}$$

Digitalni pečat (2/2)

- češće se koristi obrnuti postupak:
  1. digitalno se potpiše poruka
  2. poruka s potpisom se kriptira slučajno generiranim tajnim ključem *K*
  3. na kraju se dodaje kriptirani ključ javnim ključem primatelja
- digitalni pečat je digitalna omotnica s potpisanom porukom:

$$E\{\,[\,m;\ \underbrace{E(H(m), S_A)}_{\text{digitalni potpis}}\,],\ K\,\};\ \ E(K, P_B)$$

Autentifikacija poruka

algoritam	autentičnost	tajnost	neporecivost	integritet
MAC HMAC	+ *			+
EtM, E&M, MtE GCM	+ *	+		+
autentifikacijsko kriptiranje	+ *	+		+
digitalna omotnica		+		
digitalni potpis	+		+	+
digitalni pečat	+	+	+	+

* ne autentificira pošiljatelja već jamči da je poruku poslao „onaj koji ima tajni ključ”

4.3. Sigurnosni protokoli

Razmjena ključeva

Raspodjela ključeva

Autentifikacijski protokoli

Sigurnosni protokoli

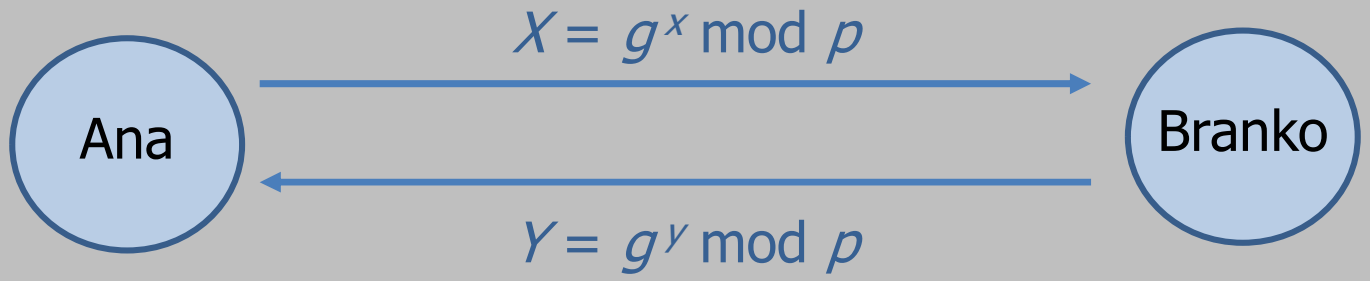
Diffie - Hellmanov postupak

- služi za razmjenu tajnog ključa
- Ana i Branko se unaprijed slože o dva vrlo velika broja n i g:
- $$\text{nzd}(g, n) = 1$$
- najpraktičnije: za n odabrati veliki prosti broj p
- g i p se mogu javno objaviti
- Ana odabire veliki nasumični prirodni broj x i šalje Branku:

$$X = g^x \bmod p$$

- Branko odabire veliki nasumični prirodni broj y i šalje Ani:

$$Y = g^y \bmod p$$



- Ana dobiva Y i izračuna zajednički ključ:

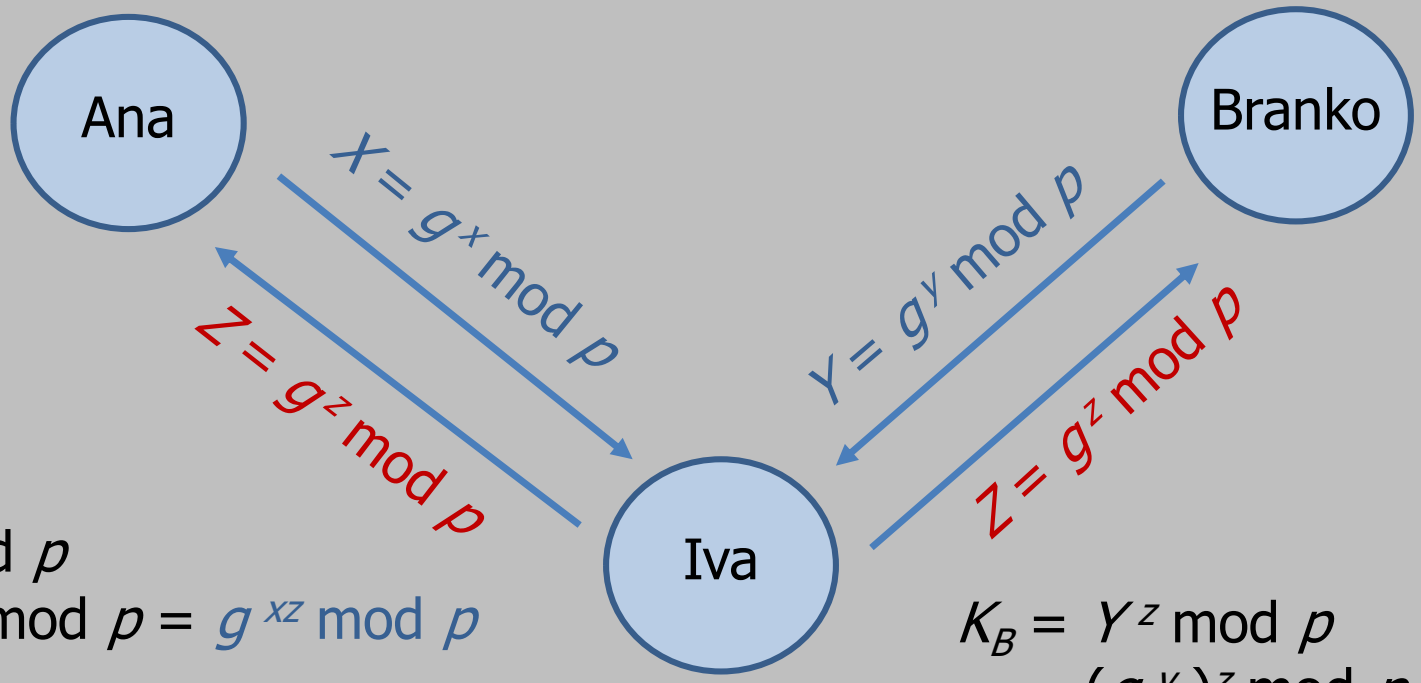
$$K = Y^x \bmod p = (g^y)^x \bmod p = g^{xy} \bmod p$$

- Branko također:

$$K = X^y \bmod p = (g^x)^y \bmod p = g^{xy} \bmod p$$

Napad *čovjek u sredini* (engl. *man in the middle*)

- napadač komunicira s Anom i Brankom (lažno se predstavljajući) uz pomoć dva ključa K_A i K_B



$K_A = X^z \bmod p$
$= (g^x)^z \bmod p = g^{xz} \bmod p$

$K_B = Y^z \bmod p$
$= (g^y)^z \bmod p = g^{yz} \bmod p$

Raspodjela ključeva u zatvorenom simetričnom kriptosustavu

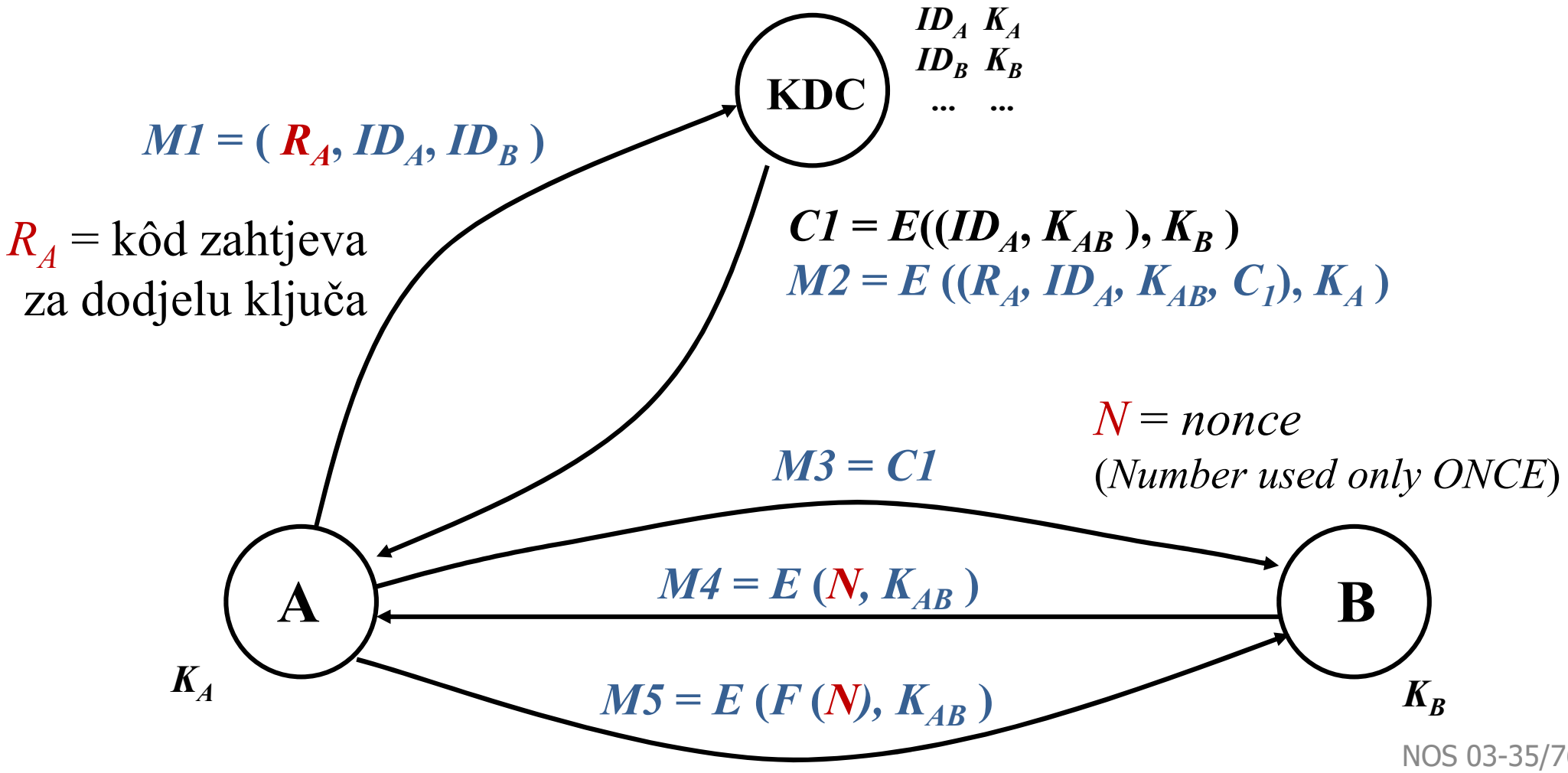
Raspodjela ključeva prema Needhamu i Schroederu

- za N sudionika: ukupno $N(N-1) / 2$ tajnih ključeva i svaki sudionik bi morao pohraniti $N - 1$ ključeva $\Rightarrow$ ozbiljno je ugrožena sigurnost!
- rješenje: pouzdani poslužitelj u kojem imaju svi povjerenje

Centar za raspodjelu ključeva (*Key Distribution Center - KDC*)

- potencijalni sudionici moraju se unaprijed prijaviti
- dodjeljuje im se tajni ključ za komuniciranje s KDC
- KDC obznanjuje identifikatore svih prijavljenih sudionika a zadržava u tajnosti pripadnu tablicu tajnih ključeva

Raspodjela ključeva u zatvorenom simetričnom kriptosustavu



Raspodijeljena raspodjela ključeva u zatvorenom simetričnom kriptosustavu